UCHWAŁA NR 97/2023
SENATU UNIWERSYTETU WROCŁAWSKIEGO
z dnia 26 kwietnia 2023 r.

w sprawie programu *Studiów Podyplomowych Zarządzanie cyberbezpieczeństwem w praktyce*

Na podstawie art. 28 ust. 1 pkt 11 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. 2022 poz. 574, z późn. zm.) uchwala się, co następuje:

§ 1. Senat Uniwersytetu Wrocławskiego ustala program *Studiów Podyplomowych Zarządzanie cyberbezpieczeństwem w praktyce* od roku akademickiego 2023/2024 w brzmieniu określonym w załączniku do uchwały.

§ 2. Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Senatu UWr
Rektor: *prof. R. Olkiewicz*

Załącznik do uchwały Nr 97/2023 Senatu Uniwersytetu Wrocławskiego z 26 kwietnia 2023 r.

PROGRAM
Studiów Podyplomowych Zarządzanie cyberbezpieczeństwem w praktyce

Program studiów obejmuje 2 semestry i zakłada 226 godzin dydaktycznych.
Łączna liczba punktów ECTS: 74.
Po uzyskaniu wszystkich zaliczeń słuchacze przystępują do egzaminu końcowego.

SEMESTR I					
Lp.	Nazwa przedmiotu	Liczba godzin	Forma zajęć	Forma zaliczenia	Punkty ECTS
1.	Wprowadzenie do cyberbezpieczeństwa i zarządzania operacyjnego w organizacji	2	wykład	zaliczenie (zal)	1
2.	Rola i zadania osób odpowiedzialnych za bezpieczeństwo (*Chief Security Officer*, *Chief Information Officer* i *Chief Information Security Officer*)	2	wykład	zaliczenie (zal)	1
3.	Zarządzanie strategiczne cyberbezpieczeństwem	4	wykład	zaliczenie (zal)	1
4.	Architektura cyberbezpieczeństwa	2	wykład	zaliczenie (zal)	1
5.	Aspekty operacyjne cyberbezpieczeństwa (zapobieganie, wykrywanie, odpowiedź)	4	warsztaty	zaliczenie (zal)	1
6.	Zarządzanie operacyjne	26	warsztaty	zaliczenie (zal)	8
7.	Zarządzanie inwestycjami w cyberbezpieczeństwo	8	wykład	zaliczenie (zal)	3
8.	Ubezpieczenia ryzyk cyber	4	wykład	zaliczenie (zal)	1
9.	Współpraca z doradcami zewnętrznymi	4	wykład	zaliczenie (zal)	1
10.	Kluczowe wskaźniki efektywności (KPI) a zarządzanie cyberbezpieczeństwem	2	wykład	zaliczenie (zal)	1
11.	Wprowadzenie do informatyki śledczej	4	wykład	zaliczenie (zal)	1
12.	Stres w miejscu pracy i radzenie sobie z nim	4	warsztaty	zaliczenie (zal)	1
13.	Wprowadzenie do sieci komputerowych	2	wykład	zaliczenie (zal)	1
14.	Inżynieria systemowa	2	wykład	zaliczenie (zal)	1
15.	Chmura obliczeniowa (cloud computing) i usługi w chmurze	2	wykład	zaliczenie (zal)	1
16.	Bezpieczeństwo wiodących systemów operacyjnych i aplikacji www	2	wykład	zaliczenie (zal)	1
17.	Urządzenia mobilne	2	wykład	zaliczenie (zal)	1
18.	Internet rzeczy (IoT)	2	wykład	zaliczenie (zal)	1
19.	Praca zdalna	2	wykład	zaliczenie (zal)	1
20.	Praktyczne aspekty informatyki i prawa	4	wykład	zaliczenie (zal)	1
21.	Organy korporacji i organizacja ich funkcjonowania	2	wykład	zaliczenie (zal)	1
22.	Współpraca z organami nadzorczymi oraz organami ścigania i wymiaru sprawiedliwości	2	wykład	zaliczenie (zal)	1

23.	Procedury na wypadek kontroli organów państwowych	4	warsztaty	zaliczenie (zal)	1
24.	Zgłaszanie nieprawidłowości (sygnaliści)	4	wykład	zaliczenie (zal)	1
25.	Ryzyka regulacyjne w obszarze nowych technologii	4	warsztaty	zaliczenie (zal)	1
26.	Standaryzacja i certyfikacja w zakresie cyberbezpieczeństwa (ISO 27000, ISO 22301, ISO 27036, standardy NISO, CSF, Polskie Normy). Część I	4	wykład	zaliczenie (zal)	1
27.	Seminarium dyplomowe	8	seminarium	zaliczenie (zal)	3
				RAZEM	38

SEMESTR II					
Lp.	Nazwa przedmiotu	Liczba godzin	Forma zajęć	Forma zaliczenia	Punkty ECTS
1.	Krajowy system cyberbezpieczeństwa	4	wykład	zaliczenie (zal)	1
2.	Cyberbezpieczeństwo a systemy com-pliance	4	wykład	zaliczenie (zal)	1
3.	Ochrona informacji poufnych i tajemnicy zawodowej	4	wykład	zaliczenie (zal)	1
4.	Ochrona danych osobowych	4	wykład	zaliczenie (zal)	1
5.	Ochrona informacji niejawnych. Bezpie-czeństwo teleinformatyczne	4	wykład	zaliczenie (zal)	1
6.	Audytor wiodący systemu zarządzania bezpieczeństwem informacji	12	wykład	zaliczenie (zal)	4
7.	Standaryzacja i certyfikacja w zakresie cyberbezpieczeństwa (ISO 27000, ISO 22301, ISO 27036, standardy NISO, CSF, Polskie Normy). Część II.	8	warsztaty	zaliczenie (zal)	3
8.	System zarządzania bezpieczeństwem informacji	8	wykład	zaliczenie (zal)	3
9.	Cyberbezpieczeństwo usług kluczowych	12	wykład	zaliczenie (zal)	3
10.	Cyberprzestępczość	4	wykład	zaliczenie (zal)	1
11.	Cyberterroryzm	4	wykład	zaliczenie (zal)	1
12.	Wybrane aspekty z zakresu zamówień publicznych	4	wykład	zaliczenie (zal)	1
13.	Opracowywanie procedur wewnętrznych	4	warsztaty	zaliczenie (zal)	2
14.	Pełnomocnik ds. cyberbezpieczeństwa	4	wykład	zaliczenie (zal)	1
15.	Podstawy kryptografii i podpisy cyfrowe	4	wykład	zaliczenie (zal)	1
16.	Shadow IT	4	wykład	zaliczenie (zal)	1
17.	Systemy automatyki przemysłowej	2	wykład	zaliczenie (zal)	1
18.	Blockchain i kryptowaluty	4	wykład	zaliczenie (zal)	1
19.	Sztuczna inteligencja	2	wykład	zaliczenie (zal)	1
20.	Bankowość elektroniczna	2	wykład	zaliczenie (zal)	1
21.	Wojna informacyjna i hybrydowa	4	wykład	zaliczenie (zal)	1

22.	Nowe zagrożenia w zakresie cyberbezpieczeństwa	4	wykład	zaliczenie (zal)	1
23.	Seminarium dyplomowe	8	seminarium	zaliczenie (zal)	3
				RAZEM	35

OPIS ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ DLA STUDIÓW PODYPLOMOWYCH

Wydział Prawa, Administracji i Ekonomii Studia Podyplomowe Zarządzanie Cyberbezpieczeństwem w Praktyce Poziom kwalifikacji cząstkowej: 7		
Kod efektu uczenia się dla studiów podyplomowych	**Efekty uczenia się**	Odniesienie do charakterystyk drugiego stopnia PRK
WIEDZA		
SP_W01	Ma pogłębioną wiedzę o miejscu i specyfice zarządzania cyberbezpieczeństwem w otoczeniu gospodarczym, z uwzględnieniem regulacji prawnych, standaryzacji procesów zarządzania zgodnością, w tym zwłaszcza odpowiednich norm branżowych.	P7S_WG
SP_W02	Rozumie istotę i funkcje zarządzania cyberbezpieczeństwem w praktyce organizacji.	P7S_WG
SP_W03	Zna w pogłębionym stopniu instytucje funkcjonujące w zakresie zarządzania cyberbezpieczeństwem, a także ich zastosowanie do realizacji celów biznesowych zgodnych z przepisami prawa, kodeksami branżowymi, procedurami i regulacjami wewnętrznymi oraz zasadami etyki.	P7S_WG
SP_W04	Zna zasady funkcjonowania oraz rolę osób odpowiedzialnych za cyberbezpieczeństwo oraz auditora wewnętrznego.	P7S_WK
SP_W05	Zna wymagania regulacyjne i etyczne w zakresie funkcjonowania cyberbezpieczeństwa w organizacji.	P7S_WG
UMIEJĘTNOŚCI		
SP_U01	Formułuje złożone pisemne oraz ustne wypowiedzi w zakresie audytu wewnętrznego, uwzględniające relacje z otoczeniem prawnym i regulacyjnym, jak również potrafi dostosować działania firmy do wymogów cyberbezpieczeństwa.	P7S_UW
SP_U02	Identyfikuje złożone problemy w zakresie cyberbezpieczeństwa oraz rozwiązuje je posługując się właściwym instrumentarium, w tym prawnym, jak również potrafi projektować systemy zarządzania ryzykiem.	P7S_UW
SP_U03	Potrafi opracować procedury cyberbezpieczeństwa i audyt wewnętrzny oraz wdrożyć oraz monitorować mechanizmy oraz programy polegające na zapobieganiu i przeciwdziałaniu ryzykom cyber w organizacji.	P7S_UK
SP_U04	Dostrzega konsekwencje zastosowania określonych regulacji prawnych w danym stanie faktycznym projektując procedury w zakresie cyberbezpieczeństwa oraz przeprowadzając audyt wewnętrzny.	P7S_UO
SP_U05	Posiada w pogłębionym stopniu umiejętności interpersonalne w zakresie rozwiązywania problemów z zakresu cyberbezpieczeństwa lub przeprowadzania audytu wewnętrznego.	P7S_UU
SP_U06	Sprawnie posługuje się przepisami prawa w codziennej praktyce zawodowej z zakresu cyberbezpieczeństwa oraz	P7S_UW

	potrafi monitorować system zarządzania cyberbezpieczeństwem.	
KOMPETENCJE SPOŁECZNE		
SP_K01	Dostrzega konieczność ciągłego doskonalenia i aktualizacji wiedzy z zakresu cyberbezpieczeństwa.	P7S_KK
SP_K02	Jest gotów podjęcia pracy jako Chief Security Officer, Chief Information Officer, Chief Information Security Officer, auditor wewnętrzny, specjalista ds. zarządzania cybezbezpieczeństwem, jak również pracownik działu audytu, kontroli wewnętrznej, bezpieczeństwa, zarządzania ryzykiem.	P7S_KO
SP_K03	Podkreśla znaczenie rozwoju wiedzy o cyberbezpieczeństwie oraz zastosowaniu jego instytucji w kontekście zmian gospodarczych i społecznych.	P7S_KR

Objaśnienie symboli:
PRK – Polska Rama Kwalifikacji
P6S_WG/P7S _WG – kod składnika opisu kwalifikacji dla poziomu 6 i 7 w charakterystykach drugiego stopnia Polskiej Ramy Kwalifikacji
SP_W - kierunkowe efekty uczenia się w zakresie wiedzy
SP_U - kierunkowe efekty uczenia się w zakresie umiejętności
SP_K - kierunkowe efekty uczenia się w zakresie kompetencji społecznych
01, 02, 03 i kolejne - kolejny numer kierunkowego efektu uczenia się